

UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

IN THE MATTER OF THE SEARCH OF:
8 JENNINGS DRIVE
BENNINGTON, VERMONT

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED
2019 AUG 30 AM 9:40
CLERK
LAW
BY
Case No. 2:19-mj-147 - DEPUTY CLERK

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Caitlin Moynihan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 8 Jennings Drive, Bennington, Vermont (hereinafter "Subject Premises"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS) and the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since October 2009. I graduated from the Federal Law Enforcement Training Center in April 2010. I am currently assigned to the Burlington, Vermont Residence Office. I hold a Bachelor of Arts degree in sociology from Providence College. Throughout my time with HSI, I have gained experience, through training and everyday work, in investigating violations relating to child exploitation and child pornography.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. As a

Special Agent, I know that Title 18, United States Code, Section 2252(a)(4)(B) prohibits a person from possessing images of children engaged in sexually explicit conduct, as defined in 18 U.S.C. section 2256 (“child pornography”), Section 2252(a)(1) prohibits the transportation of child pornography, and 18 U.S.C. Section 2252(a)(2) prohibits the receipt and distribution of child pornography.

4. I believe that probable cause exists to believe that property which constitutes evidence of the following crimes: possession, transportation, receipt, and distribution of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A, may be found inside the premises at 8 Jennings Drive, Bennington, Vermont, as further described in Attachment A.

5. The property sought to be seized and searched is described in Attachment B.

6. I have not included in this affidavit every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to search the Subject Premises.

7. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers and witnesses, and on my experience and training as a Special Agent.

CHARACTERISTICS OF CHILD PORNOGRAPHERS

8. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have spoken, I know that there are certain characteristics common to many individuals involved in such crimes:

a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from

fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with others to share information and materials.

BACKGROUND ON NCMEC AND CYBER TIPS

9. The National Center for Missing and Exploited Children (NCMEC) is a private nonprofit corporation, incorporated under the laws of the District of Columbia. It was created in 1984, and its mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC serves five main areas: (1) missing children; (2) child sexual exploitation; (3) training; (4) safety and prevention; and (5) child victim and family

services. NCMEC operates various programs in pursuit of its mission. Among these programs is the CyberTipline.

10. The CyberTipline receives leads and tips regarding suspected crimes of sexual exploitation committed against children. The CyberTipline began in March 1998, and since its inception it has received more than 27 million reports of child sexual exploitation. The CyberTipline provides online users and Electronic Service Providers (ESP) an effective means of reporting internet related child sexual exploitation including the possession, manufacture, and distribution of child pornography, online enticement of children, and child prostitution, among others.

11. Reports to the CyberTipline are made by the public and ESPs. ESPs are required by federal law to report apparent child pornography to law enforcement via the CyberTipline. ESPs are not required by federal law to search their networks for apparent child pornography. Any United States-based company providing an electronic communication service to the public through a facility or means of interstate or foreign commerce is required to register with and report to the CyberTipline.

12. The CyberTipline reporting mechanism assists law enforcement with the detection and investigation of child sexual exploitation crimes.

INFORMATION REGARDING ENTITY¹ IMAGE SEARCH

¹ I know the name of "Entity," but am not including such information in this affidavit to protect the integrity of ongoing investigations.

13. Entity is a web search engine owned and operated by Parent Company.² Entity provides a variety of search services, including web, video, image and map search products.

14. Entity's image search product provides the ability to be able to perform a reverse image search. This is done by either uploading an image from one's computer or pasting a URL in the search area. This provides the ability to search using the visual properties of the image to find any other versions or similar images.

15. The reverse image search is a content-based image retrieval (CBIR) query technique that involves providing the CBIR system with a sample image that it will then base its search upon; in terms of information retrieval, the sample image is what formulates a search query.

16. Parent Company uses PhotoDNA to hash and convert images searched for in Entity Image Search into numerical values which are then matched against a database of hashes from known illegal images. When a match is found, it is verified by a Parent Company employee who views the image. This process allows Parent Company to identify and remove illegal content from its platforms and help protect users and young victims while helping make the Internet safer for everyone.

PROBABLE CAUSE

17. Detective Matt Raymond of the Vermont Attorney General's Office is Commander of the Vermont Internet Crimes Against Children Task Force (the ICAC). As the Commander of the Vermont ICAC, Detective Raymond receives all CyberTips from NCMEC that have been deemed to have ties to Vermont. Detective Raymond received a total of three (3)

² I know the name of "Parent Company," but am not including such information in this affidavit to protect the integrity of ongoing investigations.

CyberTip Reports (the CyberTips) from NCMEC relevant to this investigation. The three CyberTips were reported to NCMEC by Entity and were in reference to three files of suspected child pornography. Detective Raymond assigned CyberTip Report #'s 46349270, 46346577 and 46349268 to himself for initial investigation. These CyberTips were assigned together because they all involved the same IP address (73.114.124.235). I have spoken to Detective Raymond about his investigation of the CyberTips and have reviewed the CyberTips myself.

18. In reviewing CyberTip #46349270, I found:

- a. Entity reported that an image file (8e4a210c-6ee3-4ee4-b198-50a96860ea5e.jpg) was uploaded or viewed from IP Address 73.114.124.235 on February 5, 2019, at 04:48:27 UTC.
- b. A person from Entity viewed the file and classified the image as depicting a pubescent minor, depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.
- c. I have viewed the image referenced in CyberTip #46349270 and based on my training and experience, I believe that this image depicts child pornography. I describe the image further as follows: it is an image file depicting what appears to be a prepubescent female child approximately 10 to 12 years old. The female child is partially nude on a what appears to be a bed, laying on her right side. The prepubescent female child has a white tank top on; she does not have pants or underwear on. The prepubescent female child's legs are spread apart, exposing her genitals; her finger appears to be inserted in her anus. There is no visible pubic hair on the prepubescent female child. The image has a watermark in the bottom right corner which says: "underage home."

19. In reviewing CyberTip #46346577, I found:

- a. Entity reported that an image file (b9b4e6f8-450a-4369-a7bd-4393a7d982ad.jpg) was uploaded or viewed from IP Address 73.114.124.235 on February 5, 2019, at 04:49:45 UTC.
- b. A person from Entity viewed the file and classified the image as depicting a pubescent minor, depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.
- c. I have viewed the image referenced in CyberTip #46346577 and based on my training and experience, I believe that this image depicts child pornography. This image appears to be the same image described in Paragraph 18(c), above.

20. In reviewing CyberTip #46349268, I found:

- a. Entity reported that an image file (ddaa9a8d-2dd1-4e3b-92a4-d6816e3eb265.jpg) was uploaded or viewed from IP Address 73.114.124.235 on February 5, 2019, at 04:49:59 UTC.
- b. A person from Entity viewed the file and classified the image as depicting a pubescent minor, depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.
- c. I have viewed the image referenced in CyberTip #46346577 and based on my training and experience, I believe that this image depicts child pornography. This image appears to be the same image described in Paragraph 18(c) above.

21. Det. Raymond caused American Registry for Internet Numbers (ARIN) to be queried regarding IP Address 73.114.124.235 and learned that IP address is currently registered to Comcast Cable Communications (Comcast).

22. On July 3, 2019, Detective Raymond provided the above information to HSI Intelligence Research Specialist (IRS) Nancy Woods and requested that she serve a Department of Homeland Security (DHS) Summons on Comcast for subscriber information for IP address 73.114.124.235 assigned on February 5, 2019 at 04:49:00 UTC. IRS Woods served the DHS Summons on July 3, 2019 and on July 5, 2019, she received a response from Comcast Cable Communications Legal Response Center. The response provided the following information regarding the subscriber of IP address 73.114.124.235 on the above-mentioned date and time as:

Subscriber Name:	MICHELLE BARBARO
Service Address:	8 JENNINGS DR BENNINGTON, VT 05201
Telephone #:	(802) 440-5145
Type of Service:	High Speed Internet Service
Account Number:	8773500300284376
Start of Service:	10/27/2017
Account Status:	Active
IP Assignment:	Dynamically Assigned
IP History:	All available attached to date of Summons (last 180 days)
E-mail User Ids:	ladybug526868@comcast.net

23. On August 8, 2019, I received the case from Detective Raymond for additional investigation.

24. On August 8, 2019, I contacted the Vermont Department of Motor Vehicles (DMV) and asked for registered vehicles and drivers associated with the Subject Premises. The

response from DMV indicated that a V.S.³ was associated with the Subject Premises and had no vehicles registered to her. I then requested information related to Salvatore Barbaro, with a year of birth of 1981 and Michelle Barbaro with a year of birth of 1982. A response was received which indicated that Michelle Barbaro had two vehicles registered to her: a 2008 Audi, black in color, bearing VT tag: GPX134 and a Jeep Cherokee, silver in color, bearing VT tag: GTD466. The response stated that the address listed for both Michelle and Salvatore Barbaro is 1265 S Stream Road 2 in Bennington, Vermont. The response also included DMV photographs of both individuals.

a. I conducted research into V.S. and it appears that she currently resides in Massachusetts and is no longer associated with the Subject Premises.

b. I caused a further vehicle query to be done of VT tag: GPX134, which revealed that the vehicle is an Audi A3.

c. I caused a further vehicle query to be done of VT tag: GTD466, which revealed that the vehicle is a 2006 Jeep Grand Cherokee.

25. On August 8, 2019, I checked with the United States Postal Service (USPS) to ascertain who was currently receiving mail at 8 Jennings Drive in Bennington, Vermont, Vermont. On August 14, 2019, I received a response indicating that the only name that the post office knows that is receiving mail there is Barbaro.

26. On August 9, 2019, I checked with the Vermont Sex Offender Registry to ascertain whether Salvatore Barbaro, with a year of birth of 1981, was currently on the sex

³ I know the full name of V.S.; however, I am not including that name in this Affidavit, as V.S. is not suspected of any involvement in the criminal conduct discussed herein.

offender registry. I received a response indicating that Salvatore Barbaro was listed on the registry due to convictions for 50 counts of sexual abuse of children – possession of child pornography and 50 counts of sexual abuse of children – dissemination of photographs, videotapes, computer depictions and film. The response indicated that his current address is 8 Jennings Drive in Bennington, Vermont.

27. A public records report accessed through CLEAR, a public records database that can be accessed and searched over the internet for Salvatore Barbaro in Vermont revealed a possible address of 8 Jennings Drive in Bennington, Vermont. CLEAR also indicated that Salvatore Barbaro may currently be on probation or parole with the Bennington office.

28. I conducted record checks in the FBI Interstate Identification Index (III) and determined that Salvatore Barbaro has an FBI record number of: 55143MC7. I conducted record checks in the State of Vermont criminal history databases for Salvatore Barbaro and determined that he has a State of Vermont record number of: 351383.

- a. Research indicated that Salvatore Barbaro was convicted in Pennsylvania in 2006 for resisting arrest and was convicted in Pennsylvania in 2014 for sexual abuse of children.
- b. Further research indicated that the 2014 conviction for sexual abuse of children was a result of a peer-to-peer file-sharing investigation⁴ involving downloads of child pornography files.

⁴ Peer-to-peer computing or networking is when computers in a network shares access to files, eliminating the need for a centralized server. A digital investigative tactic utilized by law enforcement is to download files suspected to be child pornography from peer-to-peer networks, and use the download as a method of identifying child pornography collectors and distributors.

29. On August 20, 2019, I caused a summons to be sent to the Vermont Department of Labor requesting wage information related to Salvatore Barbaro with SSN: XXX-XX-6684. I received a response indicating that for the last eight quarters Salvatore Barbaro had no records in the system.

30. On August 22, 2019, at approximately 0528 hours, SA Mike McCullagh and I traveled to the Subject Premises, and observed two vehicles parked in the driveway. No lights inside of the residence were observed to be on at this time; a television in the front room of the residence was observed to be on. I used an openly available wireless network discovery tool to search for available wireless networks while parked in front of the Subject Premises. The program identified approximately 32 wireless networks in the area, six of which appeared to be unsecured. There was a secured network named "Ladybug" which may be associated with the Subject Premises, as the email address associated with the Comcast subscriber information outlined above was "ladybug526868@comcast.net."

31. On August 22, 2019, at approximately 0606 hours, the same two vehicles were observed parked in the driveway: a silver Jeep bearing VT tag: GTD466 and a black Audi bearing VT tag: GPX134. At this time, I took photographs of the Subject Premises.

32. On August 28, 2019, at approximately 0550 hours, SA Mike McCullagh and I traveled again to the Subject Premises, and observed two vehicles in parked in the driveway: a Jeep and an Audi. No lights inside of the residence were observed to be on at this time; a television in the front room of the residence was observed to be on. The garage door on the left was slightly open. At approximately 0607 hours, the same two vehicles were observed parked in the driveway: a silver Jeep bearing VT tag: GTD466 and a black Audi bearing VT tag: GPX134.

33. I have viewed the Subject Premises and describe it here and in Attachment A as a two-story, single family home, tan in color, with black shutters. The residence has an attached two-car garage. There appear to be two front entrances to the residence; if facing the residence from Jennings Drive. One entrance is directly to the left of the two-car garage. The number “8” is displayed to the left of this entrance. If facing the residence from Jennings Drive, the second front door is located to the left of a set of large windows.

TECHNICAL TERMS

34. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses. There are two commonly used types of IP addresses called IPv4 and IPv6. IPv4, or IP version 4, is a 32-bit numeric address that consists of a series of four numbers, each ranging between 0 and 255, that are separated by dots. An example of an IPv4 address is 123.111.123.111. IPv6, or IP version 6, is a 128-bit hexadecimal address that consists of a series of eight values separated by colons. Hexadecimal values consist of a series of numbers between 0 and 9 and letters between A and F. An example of an IPv6 address is: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- b. PhotoDNA is a technology developed by Microsoft and improved by Dartmouth College that computes hash values of images, video and audio files to identify alike images. PhotoDNA is primarily used in the prevention of child pornography, and works by computing a unique hash that represents the image. This hash is computed such that it is resistant to alterations in the image, including resizing and minor color alterations. It works by converting the image to black and white, re-sizing it, breaking it into a grid, and looking at intensity gradients or edges.
- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

- d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- e. “Child Pornography” includes any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).
- f. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).
- g. “Sexually explicit conduct” applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).
- h. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

35. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage

media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have spoken, I know the following about computers and computer technology:
 - i. Computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

Basically, computers serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

- ii. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.
- iii. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store many thousands of images at very high resolution.
- iv. The Internet affords individuals several different venues for meeting each other, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography such as email services and cloud storage. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. I believe that there is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and

passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to view or share child pornography the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either

seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

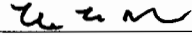
40. Because several people share the Subject Premises as a residence, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

41. I submit that this affidavit supports probable cause for a warrant to search the Subject Premises, described in Attachment A, and seize and search the items described in Attachment B.


42. I request authorization to electronically record the voices and conversations of any person present at 8 Jennings Drive, Bennington, Vermont on the day of the execution of this search warrant. An identified police officer(s) will be a knowing and consenting party/parties to the participant electronic monitoring. The participant electronic monitoring may include a digital recording made with the use of audio transmitting and receiving devices during contact with the persons mentioned above.

Respectfully submitted,



Caitlin Moynihan
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on the 30th day of August, 2019.



HON. GEOFFREY W. CRAWFORD
CHIEF UNITED STATES DISTRICT JUDGE